REMARKS/ARGUMENTS

Claims 1 to 11, 15 to 17, 20, 21, 23 and 25 have been reformatted as required by the Examiner and the first semicolon in claim 22 has changed to a colon as the Examiner required.

Claim Rejections Under 35 USC 112

Claims 1, 7 8 and 19 have been amended to eliminate the issue of the lack of antecedent basis for terms used in those claims. The applicant's attorney has also reviewed the claims for informalities and corrected the claims where necessary.

Claim Objections

The present application provides a method for creating, storing and reading a new certificate type for certification of keys. In the new certificate type, several certificates, containing redundant data fields, are collated to form one certificate and repetition of redundant information on the certificates is eliminated by use of a group or basic certificate. The group certificate is used where several keys are to be issued at the same time for the same user by the same certification authority. By means of the group certificate, repetition of all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate. This substantially reduces the memory requirement, and handling of the certificates is simplified for the communication partners. A particular embodiment of the new certificate types are the basic and supplementary certificate combination. This form of certification is used where certificates are

issued at different times for the same user by the same certification body. The memory requirement is consequently somewhat more than for group certificates, but greater flexibility is gained in use of the keys. The applicantion discloses a configuration once methodoloy of use of the group or basic and supplementary certificates that enable their use in the number of differernt situations.

Claim Rejections Under 35 USC 103

A. Claims 1 to 12 were rejected under 35 USC 103(a) as being unpatentable over VeriSign "Certificate Practice Statement", version 1.2, in view of Sutter, U.S. patent #5,924,094, Stallings "Cryptography and Network Security", 2nd Edition, and Karlton "Proposal to Add Attribute Certificates to TLS 3.1".

Applicant's attorney found nothing in the recited combination that teaches combining redundant information for several keys into one group certificate and then issuing supplementary certificates for each of the several keys. With respect to supplementary certificates, the Examiner points out that VeriSign does not teach the use of a supplementary certificates for the issuance of additional keys and relies on the teachings of the Sutter patent and the Karlton reference to provide the missing teaching. However, the subject matter cited in the Sutter patent does not mention supplementary certificates and Karlton clearly states that what is described as an "attribute cert" shall have no associated key pair and cannot be used to establish identity. Therefore, the Karlton teaching specifically excludes use of its attribute cert for applicant's purposes. Accordingly, there not only is a lack of teaching applicant's invention in the proposed combination of Verisign, Sutter and Karlton, but a specific exclusion of any such teaching of the combination for the purposes

proposed by applicant in view of Karlton's express statements about configuration and limitation and use of attribute certs. Without the issuance of further keys in applicant's supplementary certificates, the advantages in accordance with the applicant's invention cannot be obtained.

As for group certificates, the Examiner points out that VeriSign does not disclose a certificate designed to carry a plurality of keys and discusses the Stallings article in this connection. However, the Examiner points out that he found nothing in the Stallings article that mentions a group certificate containing multiple keys. Therefore there is no teaching in the combination for a group certificate designed to carry multiple keys.

In addition to the failure of the references to disclose a proper combination of patents to meet the applicant's disclosed invention, the Examiner fails to provide evidence of any suggestions in the references or otherwise (as the time of applicant's invention) to combine and modify the references as suggested by the Examiner. The reasons that the Examiner gives for it being obvious to make the combination the Examiner proposes essentially breaks down to the need for applicant's invention. That is, it appears that what the Examiner is saying is that in view of this need, those skilled in the art would go through the numerous references in the field, pick out the same four the Examiner has chosen, then modify them just as the Examiner has done and then combine them so as to meet every detail in every one of the 25 claims of the application. This is an unlikely scenario. It appears that what the Examiner has done in his rejection is use hindsight to select certain, otherwise unconnected, references out of a multiplicity of such references and then piece them together and modify them using the applicant's disclosure as an

instruction manual and the claims in the application as templates to piece together the teachings of these modified prior art references.

B. Claims 13 to 18 were rejected under 35 USC 103(a) in view of the combination cited in A further in view of the Deo, U.S. patent #5,721,781.

The addition of the Deo patent to the combination cited in A does not change the failure of the combination cited by the Examiner in A to teach applicant's invention. Further, the cited sections of Deo do not specifically teach storing a basic and/or supplementary certificate in a nonvolatile memory of a chip card. Claims 15 to 17, cited in this section, are not limited to a chip card.

C. Claims 19 to 25 were rejected over the prior art cited against claims 1 to 7 in A further in view of "JAVA XZ509 Certificates and Certificate Revocation Lists." The arguments presented in A with respect to claims 1 to 7 apply equally well to the Examiner's position with respect to rejection of claims 19 to 25 in B and C.

The Claims

The claims in the application are all allowable for the reasons given above. Independent claims 1, 8, 10 and 19 are all limited either to the combination of sequential and supplementary certificates, as discussed above, or to one of the or other of the certificates. For instance:

Claim 1 calls for a method requiring creation of both a basic certificate and a supplementary certificate for one key and then using the basic certificate for future keys that share redundant information with the basic certificate.

Claim 8 calls for generation of a single group certificate for several keys with all data elements necessary for all keys and key pairs generated in step A with group certificates containing only a single recitation of data elements redundant to all the keys.

Claim 10, like claim 1, calls for definition of both a basic certificate and a supplementary certificate with one of the keys of a generated key pair inserted into the supplementary certificate.

Claim 19 recites a computer program product containing a basic certificate and at least one supplementary certificate and using the basic certificate with future keys that share the redundant information with the basic certificate by issuing an additional supplementary certificate with a key from a new key pair.

Dependent claims further distinguish over the prior art in that they recite further steps or structure not found in the prior art. For instance:

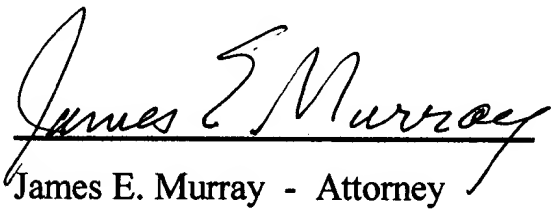
Claims 2, 3, 4, 7, 9, 11, 20, 21, 23 and 25 recite data elements for either the basic or supplementary certificates recited in one or the other of the independent claims. Since there is no supplementary or basic certificates defined by the prior art, these combinations are not taught by the prior art.

Claims 4, 6, 15, 16, 17, 22 and 24 relate to steps involved to determine if a basic certificate exists and steps to be taken if one or more keys to be certified at one time.

Claims 13, 14 and 18 further distinguish in that they call for the basic and supplementary chips to be stored in the nonvolatile memory of a chip card.

For the above reasons, the application is in condition for allowance and it is therefore respectfully requested that it be reconsidered, allowed to passed to issue.

Respectfully submitted,



James E. Murray - Attorney
Reg. No.: 20,915
Telephone No.: (845) 462-4763